TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF AUTHORITIES

FEDERAL CASES

TABLE OF CONTENTS

I. INTRODUCTION

The InterTrust patent claims' use of the vague term "secure" and its variants makes them textbook illustrations of the danger of indefinite claims. Without a definition of this malleable core term, persons of skill in the art cannot determine the scope of patent coverage. This is precisely the situation prohibited by 35 U.S.C. § 112's requirement of "particularly pointing out and distinctly claiming" the alleged invention. The purpose of the claims is to define the metes and bounds of the exclusive right that the public grants in exchange for the patentee's full disclosure. Where those boundaries are blurry, others are deterred from entering the field, allowing the patentee to exclude competition beyond the scope of the claimed invention. The InterTrust patent claims using "secure" and its variants violate the bargain with the public in this fashion, and should be found fatally indefinite and, therefore, invalid.

InterTrust's testifying expert concedes that "security" is an "essential aspect" of the "invention," InterTrust's so-called "Virtual Distribution Environment" ("VDE"). Declaration of Eric L. Wesenberg, Ex. A, Reiter Depo., 23:21-24:9.[1] "Secure," or some close derivative thereof, appears in virtually every disputed claim. Reading Claim 1 of U.S. Patent No. 5,892,891 ("the '891 patent") demonstrates the extensive use of the vague term "secure":

> A method for using at least one resource processed in a **secure operating environment** at a first appliance, said method comprising: **securely receiving** a first entity's control at said first appliance, said first entity being located remotely from said operating environment and said first appliance; **securely receiving** a second entity's control at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and **securely processing** a data item at said first appliance, using at least one resource, including **securely applying**, at said first appliance, through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item. (Emphases added.)

Ex. P, Claim 1. This claim uses four different, and five total, instances of this term or its variant. Neither the claims nor the rest of the patents define what it means for something to be "secure" or to be done "securely." "Secure," in the art, is a highly general, relative and multifaceted term

[1] Hereinafter, all cites to exhibits ("Ex.") are to exhibits attached to the Declaration of Eric L. Wesenberg in support of Microsoft's Motion for Summary Judgment that Certain "Mini-*Markman*" Claims are Invalid for Indefiniteness.

which, without more specific definition, fails to have a clear or even useful meaning. In all their hundreds of pages of single-spaced description, the patents never clearly or consistently define "secure," nor the composite terms using secure (*e.g.*, "secure container"), nor the related coined terms deriving from the same concept: "protected processing environment" and "host processing environment."

The extrinsic evidence – both testimonial and documentary, both Microsoft's and InterTrust's – is in complete agreement: "secure" corresponds to a general concept in the computer field, which lacks specific meaning and standing alone may apply to numerous specific scenarios depending on the properties to be "secured," the particular threats posed, the means used, the degree of protection needed, the perspective from which one views "security," and so on.

Both parties' experts have testified that "secure" can take on a definite meaning within the context of a "security policy," which defines the parameters and sets objective criteria for determining whether they have been satisfied. Computer scientists have developed a number of models for objectively evaluating the security of different systems and architectures, at least one of which is mentioned (TCSEC), but not employed, in InterTrust's '193 patent.[2] InterTrust could easily have defined a security policy using any of these models. Instead, it left "secure" inscrutable throughout the patents.

The problem is not that it's difficult to discern the true meaning of these claim terms. It is impossible. For the reasons set forth herein, Microsoft asks that the Court find the claims containing "secure" (including its variants), "protected processing environment" or "host processing environment" invalid for indefiniteness.

///

///

///

[2] For efficiency, all references to "the specification" are to the specification of U. S. Patent No. 6,253,193 ("the '193 patent") (Ex.Q). The '193 specification reproduces, nearly identically, the "big book" original application (the original 900+ page application filed in 1995). Each of the patents at issue herein either expressly reproduce the same text in their specifications, or attempt to incorporate it by reference (though not successfully, *see infra* § II. D.).

II. FACTS

A. "Secure" Lacks a Clear Meaning in the Art.

The most pervasive indefinite term in the InterTrust patents is "secure" in all its various forms. Indeed, the provision of "security" while enabling the flexible distribution of digital information is the stated goal of the entire invention. To construe "secure," the Court must look to the ordinary meaning (if one exists) that would be attributed to the term by a person of skill in the art. *Tex. Digital Sys. v. Telegenix, Inc.*, 308 F.3d 1193, 1202 (Fed. Cir. 2002). The intrinsic and extrinsic evidence, including InterTrust's own statements and those of its expert, establish that while communicating a general or conceptual meaning, the term "secure" lacks a any precise, uniform definition to inform a person of skill in the art what it means unless a number of questions are answered. Because InterTrust never provides the needed answers, it is impossible to determine the scope of the claims.

"Secure memory" for instance, is no clearer a phrase than a "secure car." At first blush, one hearing the phrase "secure car" might think of a car equipped with features that make it difficult or impossible to steal, such as a club, an alarm siren, and or an ignition "kill switch." Only later in the conversation, hearing the speaker refer to bulletproof glass, shielded wheels, and reinforced doors would the listener realize that "secure" means something entirely different: The car is in fact designed to protect passengers from attack (to transport diplomats and heads of state). Even after the type of security is identified, different particular combinations of security measures will qualify the car as "secure" in the eyes of different customers. Simply referring to a car as "secure" fails to delineate the objective of that security, the type of security needed or the measures used to achieve it. Nor does the descriptor "secure" disclose the perspective from which "security" is being assessed. A parking enforcement officer might consider a booted vehicle "secure" (*i.e.*, from removal by its owner), while the owner might view it as "insecure" since it allowed someone to tamper with its wheels. Another variable might be the length of time the car would have to withstand the measures it is designed to resist. From this simple metaphor, the relative, multifaceted and undefined character of "secure" is readily apparent.

What is true in the vernacular applies with even greater force in the computing arts – "secure" needs definition along multiple axes to have a precise meaning. Deponents skilled and experienced in the field have spoken on this point. InterTrust's own expert, Dr. Michael Reiter, testified that "'secure' is a fairly general term that's used in the art for -- in several different ways." Ex. A, Reiter Depo., at 30:11-19. Asked to describe them, Dr. Reiter responded, "Oh, my gosh. All the ways. I can enumerate several ways I can think of on the fly. I don't know that I can enumerate everything I would do if I had more time." *Id.* at 31:10-17. Microsoft's expert, Prof. John Mitchell, agrees, identifying ten different variables (discussed below) that must be known to determine what is meant by "secure." Declaration of John Mitchell in Support of Microsoft's Motion Summary Judgment that Certain "Mini-*Markman*" Claims are Invalid for Indefiniteness ("Mitchell Decl.") at 8-11. Others involved in this industry, including some who have done, or do, business with InterTrust have testified to similar effect:

- MusicMatch; stated that in order to know whether a system is secure, one would have to know what the content provider for that system intended, and thus "security" as it applies to a particular system might mean something completely different from the same term applied to a different system. Ex. C, Jim McLaughlin Depo., p. 55:14-25.
- Envivio; stated that "secure" "doesn't mean anything in general. It means a general concept." Ex. D, Julien Signes Depo., at 40:22-41:2. When asked whether "it would be necessary ... to look at the context of the implementation of ... security to understand whether or not a system is secure," Mr. Signes answered, "yes, of course." *Id.* at 41:3-13.
- A leading authority in the field has written that "[w]ithout a precise definition of what security means and how a computer can behave, it is meaningless to ask whether a particular computer system is secure." Ex. E, Carl E. Landwehr, "Formal Models for Computer Security," ACM Computing Surveys, v.13 no. 3 (1981).
- "When someone states that 'My computer is secure,' that statement may very well mean distinctly different things to different people." Ex. F, Taylor, *Comparison Paper Between the Bell and LaPadula Model and the SRI Model*, IEEE Symp. on Security & Privacy, 1984, pg. 195, 197.

1. **To Give "Secure" a Definite Meaning, a Number of Parameters Must Be Specified.**

John Mitchell, a Professor of Computer Science at Stanford University, has identified ten parameters that persons of skill in the art would need to know in order to have a shared understanding of the meaning of "secure" in any given instance: (1) what types of things

or actions are protected; (2) what specific things or actions are protected in the system in question; (3) what properties of those things are protected; (4) against whom; (5) against what points of attack; (6) against what kind of attack; (7) for how long; (8) to what degree of protection; (9) how is protection or the loss thereof evidenced; and (10) the perspective (or perspectives) from which "security" should be considered. Mitchell Decl., 8-11 and *passim*. To be able to evaluate whether an actual system is "secure," people of skill in the art must first reach a common understanding of each of these variables, as discussed below.

a. **What is to Be Protected? (Mitchell Questions 1 and 2)**

The first variable is, what is being protected? *See* Mitchell Decl., at 9. Is the user being protected from untrusted data, or is data being protected from untrusted users? *Id.* How "secure" is understood by people of skill in the art is influenced in the first instance by what one is trying to protect, and here the claims force them to guess. InterTrust has at least partly admitted that this is true. InterTrust objected to answering a Request for Admission that "a password-protected file is secure," on the ground that it was not told, *inter alia*, "the value of the information in the file." *See* Ex. G, InterTrust's Response to Microsoft Request for Admission 101. In InterTrust's view, in other words, the presence or absence of "security" depends on the nature of the thing to be protected. For a high-value item, a password requirement alone might not be enough to make the item "secure," while the same barrier might suffice to ensure the "security" of a low-value item.

b. **The Properties to be Protected. (Mitchell Question 3)**

The next crucial component of security is which attributes of the protected items are safeguarded. The different properties include:

- secrecy (or, "confidentiality") – maintaining the secrecy of data so that its meaning is not learned by unauthorized parties;
- integrity – ensuring that data may not be altered or destroyed by unauthorized parties;
- availability – ensuring that authorized parties can use the computers'

systems and data when desired;

- authenticity – ensuring accurate proof of the identity (or perhaps other characteristics) of the author or sender of a message or data;
- non-repudiation – preventing denial of the origination or receipt of messages by parties.

Mitchell Decl., 9-10. AOL and MusicMatch agree that security includes one or more of these components. AOL; Ex. H, Saccocio Depo., 30:8-31:16 (confidentiality, integrity, non-refutability, authentication); MusicMatch; Ex. C, McLaughlin Depo., 34:16-35:14 (integrity, authentication, non-repudiation, but not necessarily secrecy). So does InterTrust's expert, who testified that "secure" could be defined narrowly to include a single criterion, "secrecy," or in contrast, requiring satisfaction of the "Common Criteria," a multi-criteria framework for identifying security requirements and evaluating systems and whether they meet those requirements. Ex. A, Reiter Depo., 31:22-25, 32:15-20; Mitchell Decl., at 7, n. 1 (*see also* http://www.commoncriteria.org). Any one of these features alone, or any combination of them might suffice to create a "secure" system, depending on the context. The assurance of "availability" might be integral to the meaning of "secure" for one user, but not for another user with different priorities, as Dr. Reiter testified:

> Q: How about availability of information? Are you familiar with the concept of availability in...
>
> A. Sure, sure.
>
> Q. Are there some senses of the word secure where ensuring availability is required and other senses of the word secure where ensuring availability is not required?
>
> A. Yes, I'd say that's true.

Ex. A, Reiter Depo., 36:9-18 (objections and other non-substantive matter omitted).

c. **The Threats to be Protected Against (Against Whom, What Points of Attack, What Kind of Attack.) (Mitchell Questions 4, 5, and 6)**

Further crucial variables in defining "secure" are the types of attackers, the different possible points of attack, and the types of threats posed. Mitchell Decl., at 10. A system billed as "secure" against attack by outsiders might not be "secure" for a customer requiring a

system that even insiders cannot misuse, or for a customer who requires protection not against its own employees but against a category of outsiders possessing certain identified information about the system or other special resources. *See, e.g.* Mitchell Decl., at 10, 20, 31, 34 (regarding "secure memory" "secure container," "secure operating environment" etc.).

The types of threats one has in mind are essential to defining "secure." As InterTrust itself argued in response to Microsoft Request for Admission that "a password-protected file is secure," one must know, *inter alia*, "the threats against which the file is to be protected." *See* Ex. G, InterTrust's Response to Microsoft Request for Admission 101. InterTrust's expert echoed this view, testifying that:

> "secure" is used as a general term to refer to protection against misuse and interference, **and to truly evaluate that security, you often need to be more precise about the sorts of misuse and interference you are concerned with, the threat models or the threats to which a system or primitive is likely to be subjected,** and the mechanism by which you protect that system.

Ex. A, Reiter Depo., 33:17-34:5 (emphasis added).

d. The Duration and Degree of Protection. (Mitchell Questions 7 and 8)

The duration and degree of protection are also prerequisites to understanding the meaning of "secure" in the art. Mitchell Decl., at 10-11. Withstanding an hour-long attack, or an attack employing a certain level of computing power might be sufficient in one context, but not another. Mitchell Decl., at 10. As to degree of protection, America Online's Director of Rich Media agreed that some notion of degree is needed to understand "secure":

> Q: But they [the criteria for "security"] can be met sufficient so that it's meaningful within this industry to use the term "secure," can they not?
>
> A: It's a vague term. I know it's frustrating, but it is. Security is a vague term. How much security is a better question.

Ex. H, Deposition of Damian Saccocio, 40:12-17.

///

///

e. How Protection is Verified and Evidenced. (Mitchell Question 9)

"Security" also depends on the manner in which continued protection, or the loss thereof, is or is not measured, tested, proven or evidenced analytically. Mitchell Decl., 11.

f. From Whose Perspective the System Is "Secure." (Mitchell Question 10)

Finally, the perspective from which "security" is viewed is crucial. A system can be "secure," or not, to a content owner, the system administrator, and or the authorized users. Mitchell Decl., at 11. Take for example, the case of a user who downloads a music file for a fee, which she pays electronically, using her credit card. If a third party tries to intercept the credit card information and make an additional, free copy of the downloaded file for himself, different outcomes could be viewed as "secure" by the different parties to the transaction. If the third party successfully copies the file, but not the credit card information, then the system might be considered "secure" from the perspective of the customer, but not the vendor. If, on the other hand, the attacker fails to copy the file, but does obtain the credit card information, and the system merely detects the unauthorized intrusion, then the vendor might consider the system "secure" while, from the customer's perspective, it is "insecure" – or at least the customer will see it that way, if she later learns of the theft.

B. The InterTrust Applicants Could Have Used the Claims or Specification to Adequately Define "Secure" But Failed to Do So.

1. InterTrust Has Not Defined "Secure" in the Claims or the Specification.

InterTrust could have chosen to define the term "secure" but didn't. Ten of the twelve claims at issue employ the word "secure" in some form, yet none of them defines it. Ex. J, JCCS Ex. H. They establish no security policy and no criteria that would answer the ten questions discussed above.

///

///

///

2. **"Secure" Remains Indefinite Even When the Claim is Viewed in Light of the Specification.**

Though "secure," and its variants, as used in the claims, lack requisite definiteness, the claims could still be saved from indefiniteness if "those skilled in the art would understand the scope of the claim when the claim is read in light of the rest of the specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir. 2001). Far from curing the problem, however, the patent specification compounds it. It contains no uniform security policy, no uniform criteria for security, and no glossary. It uses "secure" and "security" in multiple, vague and inconsistent senses, giving the potential entrant into the field no more clarity than do the claims alone.

a) **The Specification Describes Multiple Perspectives from which "Secure" Might Be Measured, and Indexes "Secure" to the Unpredictable Needs of Different Users**

The specification uses "secure" in a fashion that is impossible for a person of skill in the art to understand because it depends on the unpredictable and varying needs of potential customers. In other words, "secure" cannot be defined completely by looking at the patent documents in light of the art. Instead, the '193 specification (Ex. Q) defines "secure" in terms of whatever the market may be seeking, which changes over time and has no fixed technological meaning:

- The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. ('193 at 49:59-62)
- "a "sufficiently" secure (for the intended applications) environment" ('193 at 45:23-24)
- "with sufficient security (sufficiently trusted) for the intended commercial purposes" ('193 at 45:43-45)
- Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. ('193 at 15:67-16:5).

b) **The Specification Mentions Different and Inconsistent Secure Properties**

The specification suggests several different security properties denoted by "secure" without committing to any of them. For example, "secure" could mean that an item or process is simply encrypted ('193 at 126:6-7), or "encrypted and tagged" (*id.* at 22:18-19), or "encrypted and authenticated" (*id* at 45:39-40), or not encrypted but "otherwise secured ... such as by employing authentication and/or error-correction" (*id.* at 63:37-39).

c) **The Specification Mentions Many Different and Inconsistent Degrees of Security**

The specification uses at least a dozen adjectives apparently identifying different "levels" of security – truly secure ('193 at 80:31, 81:14, 88:38); extremely secure ('193 at 67:21); highly secure ('193 at 22:16, 23:49, 36:9-10, 41:34, 67:19, 77:30, 104:63, 132:63, 203:66, 232:47, 233:4); commercially secure ('193 at 2:20, 47:6); adequately secure ('193 at 12:50); acceptably secure ('193 at 129:25); sufficiently secure ('193 at 9:12, 16:25, 21:48, 28:47, 49:41, 207:20, 249:51); appropriately secure ('193 at 77:16); physically secure ('193 at 13:20); sufficiently physically secure ('193 at 13:20); cryptographically secure ('193 at 202:44); continually secure ('193 at 32:4); relatively secure ('193 at 63:66); non-secure ('193 at 26:22, 49:10, 62:44, 73:56, 78:16, 77:43, 80:13, 80:20, 81:19, 120:38, 139:59, 229:20); possibly less secure ('193 at 80:33).

Though the meaning of these different degrees of security is unclear, it is evident that the degree of security, like the type of security, is a function of unpredictable factors in the marketplace outside the "world" of the patent. For instance, the patent claims that "[d]irect attack on these [cryptographic] algorithms is assumed to be beyond the capabilities of an attacker. For domestic versions of VDE 100 some of this is probably a safe assumption since the basic building blocks for control information have sufficiently long keys and are sufficiently proven." '193 at 221:12-17. But what was "sufficiently long" in 1995 may not be sufficiently long now or five years from now – that is a function of changes in the larger security environment. Elsewhere, the specification promises that "the VDE 100 provided by the preferred embodiment has sufficient

security to help ensure that it cannot be compromised short of a successful 'brute force attack,' and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived." Ex. Q, '193 at 199:38-47. But the relationship between the cost of a "brute force attack" (essentially an attack that tries all possible keys no matter how long it takes) and the "value to be derived" by cracking a given system depends on the characteristics of the parties involved and changes in technology, which are "outside" the patent. The patent describes "secure" not in terms of technological means but in terms of ever-changing marketplace factors.

d) The Specification Mentions Different and Inconsistent Security Methods

Throughout the patent, different measures are described as possibly sufficient for security, but no indication is given of which measures are necessary to security:

- "a secure enclosure, such as a tamper resistant metal container or some form of a chip pack containing multiple integrated circuit components" ('193 at 169:7-10)
- "In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information" ('193 at 59:55-58)

The attached declaration of Professor John Mitchell provides many more examples of the vague, multiple and inconsistent uses of "secure" and its variants in the patent specification. Mitchell Decl. at 12-17.

C. <u>The Prosecution History Does Not Give Secure a Clear Meaning</u>.

There is nothing in the prosecution history of any of the seven patents that resolves any of the problems discussed above. The prosecution histories do not offer any definition, criteria, or aid of any kind to help one of skill in the art understand what is meant by the term "secure" and its variants in the claims. Moreover, to the extent the continuation-in-part patents criticize the "big book" application as NOT teaching how to defend against a given threat (for example, "bogus load modules" that can "wreak havoc," (Ex. R, U.S. Patent No. 6,157,721 ("'721") '721 at 7:37, 8:16)), they raise even more questions about what "secure" could possibly mean in these claims.

D. Indefiniteness of Certain Patent Claims is Highlighted by Errors Made In The Specifications

1. The '683, '721 & '861 Patents Failed to Properly Incorporate the "Big Book" by Reference

An outside publication can be made part of a patent by referring to it, rather than actually reproducing its text. *See In re de Seversky*, 474 F.2d 671 (C.C.P.A. 1973). Whether material has been "incorporated by reference" is a question of law. *Advanced Display Systems, Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). "Essential" material (*i.e.*, that which is necessary to describe the claimed invention) may only be incorporated by reference to an issued U.S. Patent or a published U.S. Patent Application. This requirement eases the burden on the public reviewing the patent, as it makes essential material readily available, whereas non-published material, like patent applications may not be available, or must be ordered at a considerable expense from the patent office. *See e.g.*, MPEP § 608.01 (p).

"The big book" material is "essential" in U.S. Patent No. 6,185,683 ("'683") (Ex. S) the '721, and U.S. Patent No. 5,920,861 ("'861") (Ex. V). In each of the patents, the "big book" is relied on to explain fundamental portions of the claimed inventions. *See* '721 at 4:51-60; '861 at 2:37-39; and '683 at 27:1-16.

2. None Of The Patents Met The "Incorporation By Reference" Requirements

The '683, '721, and '861 patents all purport to incorporate the "big book" by reference to the unpublished patent *application*. '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11. They never amended their specifications to properly reference the issued patent number. This failure means that the "big book" materials are not part of the '721, '683 or '861 patents. Therefore, any need for definitions therefrom renders the claims and patents indefinite and invalid.

E. InterTrust Failed to Fulfill Its Obligation to Define the Claim Term "Secure" as Clearly as Possible.

The extrinsic evidence, including InterTrust's own documents, indicates that it had the opportunity to be more precise. In this regard, InterTrust not only failed to apprise what the

bounds of the claim were, but also failed to be as precise as the subject matter permits. It is implicit in the lengthy discussion of parameters above that the term "secure" can be used with clear meaning in this field only after all the questions are answered. Typically this takes the form of a "security policy" and "criteria" for measuring satisfaction of that policy. A "security policy" answers "secure for whom?" and "secure for what purposes?" The security policy defines what is being protected against what attacks or threats (questions 1-6 of Mitchell Decl.). "Criteria" are designated as objective measurements for determining whether a real system satisfies the security policy. (Questions 7-10 of Mitchell). Together, the security policy and criteria allow the word "secure," which otherwise is a general and merely conceptual term, to be used in a meaningful and definite manner. The InterTrust patent claims and specification contain no uniform security policy, and no uniform definition of "secure."

The need for a specific security policy and criteria is well known in the field:

> "A given system can only be said to be secure with respect to its enforcement of some specific policy." Ex. L, *Trusted Computer System Evaluation Criteria* (1985), pg. 59.
>
> *See also* Ex. M, Landwehr, Carl E. *How far can you trust a computer?*, SAFECOMP'93, Proc. of the 12th International Conf. on Compute Safety, Reliability, and Security, Poznan-Kiekrz, Poland, Oct., 1993, Janusz Gorski, ed., ISBN 0-387-19838-5, Springer-Verlag, New York, 1993.

As quoted above, InterTrust's expert, Dr. Reiter, affirmed the need to establish criteria to evaluate whether a real-world system is or is not, secure,[3] and recognized the role of a security policy in providing such criteria:

> [I]f a system has been evaluated via the common criteria, for example, to a given protection profile, this would be an example. You know, someone might say that it's secure once it's been evaluated via that framework. Ex. A, Reiter at 32:15-20.

F. **InterTrust's Proposed *Markman* Definition Confirms That "Secure" Is Indefinite.**

Although the claim construction stage of litigation is far too late to cure patent

[3] "'[S]ecure' is used as a general term to refer protection against misuse and interference, and to truly evaluate that security, you often need to be more precise about the sorts of misuse and interference you are concerned with, the threat models or the threats to which a system or primitive is likely to be subjected, and the mechanism by which you protect that system." Ex. A, Reiter at 33:23–34:5.

indefiniteness, it is telling that InterTrust did not even try to clarify the term. On the contrary, InterTrust's proposed definition of "secure" confirms its utter vagueness. InterTrust asserts that "secure" means that "[o]ne or more mechanisms are employed to ... discourage misuse of or interference with information...," and can be achieved through "tamper resistance," elsewhere defined merely as "making tampering more difficult and/or allowing detection of tampering." Joint Claim Construction Statement filed in this Court on March 14, 2003. At the same time, InterTrust proposes that "[s]ecurity is not absolute, but is designed to be sufficient for a particular purpose." Joint Claim Construction Statement, at 6. Defining a claim relative to an unspecified "particular purpose" gives rise to precisely the uncertainty that Section 112(2) seeks to avoid. Moreover, whose perspective is sufficiency to be determined from and how are the "particular purposes" of the different users to be identified? By proposing a definition of "secure" that leads to inconsistent results, depending, for example, on who gets to specify a product's purpose, or whether its design is sufficient, InterTrust's own proposed definition confirms that the term has no definite meaning.

G. Nor Is "Secure" Redeemed By The Terms It Modifies.

None of the following claim phrases has a commonly shared understanding or usage in the field: "secure operating environment," "secure container," "secure memory," "secure database," "secure execution space," "securely applying," "securely assembling," "securely processing," or "securely receiving." Mitchell Decl., at 19-51. None of these terms resembles "smart card" or "hot dog," terms in which otherwise vague and subjective adjectives are made clear by that which they modify. In contrast, "secure" as it appears in the claims receives no assistance from the terms it modifies. A person of ordinary skill in the art would have to have answers to the questions discussed above to know in what sense each of these items is "secure." Intertrust's expert, Dr. Reiter, acknowledged that describing an item as "secure" does not, for instance, apprise one of whether it is protected against, say, denial of service attacks or attacks on causal logic, or whether the availability of information is ensured, to name just a few aspects of the concept. Ex. A, Reiter Depo., at 30-32; Mitchell Decl., at 6-7.

The problem with these compound terms is made intractable with InterTrust's

argument that "secure" must have the same meaning everywhere it appears. In its *Markman* statement, InterTrust proposed defining "secure" independently for *Markman* purposes, and defining all other claim terms that incorporate it by reference to "secure". Thus, for "secure container," InterTrust proposes the definition, "a container that is Secure." *See e.g.*, JCCS, Ex. B. "Secure database," "secure execution space," "secure memory," and "secure operating environment" are all to be defined in analogous fashion. *Id.* Within InterTrust's proposed definitions of the phrases "securely applying," "securely assembling," "securely processing," and "securely receiving," the word "securely" is defined simply as "in a Secure manner." *Id.* InterTrust has bound itself to the position that all of these phrases must share a common definition of "secure." All claims containing that term, then, are indefinite and invalid.

H. INTERTRUST'S COINED TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" ARE ALSO INDEFINITE.

In its patents, InterTrust introduces the terms "Protected Processing Environment" (or "PPE") and "Host Processing Environment" (or "HPE") — InterTrust coined these terms. Recognizing that they were new, proprietary terms, InterTrust often provides initial capitalization to the phrases or sets them off by quotation marks within the specification. (*See, e.g.* Ex.Q, '193 at 9:29, 13:10, 50:40, 105:18-19, 283:46)). These coined terms also appear in several claims including some of the mini-*Markman* claims (*e.g.* Ex. S, the '683 claim 2, and Ex. R, '721 claim 34.) It is the patentee's "duty to provide a precise definition" of terms unknown to those of ordinary skill in the art. *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1570 (Fed. Cir. 1997).

1. THE TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" HAVE NO ORDINARY COMPUTING ART MEANING.

The terms "Protected Processing Environment" ("PPE") and "Host Processing Environment" ("HPE") do not have an ordinary or customary meaning inside or outside of the computing world. They have not been found in any dictionaries that Microsoft has consulted. InterTrust has offered no dictionary or other extrinsic references to provide a meaning for these terms.

Significantly, even InterTrust's testifying expert confirmed that the terms would not have a known meaning to one of ordinary skill in the art in February 1995, when InterTrust submitted the "big book" application. Regarding the term "Protected Processing Environment," Dr. Reiter testified:

> Q. ...in February 1995, would the person of ordinary skill in the art have heard of the phrase protected processing environment?
>
> A. It's not a term in the art. One might assume certain things about that, but it's not a term in the Art.

(Ex. A, Reiter Depo., 131:22-132:2). He testified similarly that a person of ordinary skill would not be familiar with the term HPE. *Id.* at 132:3-6.

Not surprisingly, third party deponents, all of which had close dealings with InterTrust (most licensees of the asserted patents) were at a loss to assign any meaning, ordinary or otherwise, to these terms. *See* Ex. D, Envivio Depo. at 53:9-19 ("Q: Have you ever heard the term "protected processing environment"? A: No."); Ex. H, AOL Depo at 82:21-92:3; 96:4-97:17.

2. THE CLAIMS DO NOT PROVIDE SUBSTANCE OR CONTEXT SUFFICIENT TO PROVIDE MEANING TO EITHER PPE OR HPE.

These coined terms are used in three of the "Mini-*Markman*" claims: PPE is found in two and HPE is found in one. The claims do not provide the necessary context to formulate a sufficiently definite meaning.

The words of Claim 2 of the '193 patent, provide little information about what is meant by PPE. While it does partially indicate what is being protected, "*in part protecting information contained*", from what, "*from tampering*" and by who, "*by a user*", it still fails to inform one of ordinary skill if it "protects" "part" of the information or is "part" of the "protection". Also left open is what partial protection from tampering means. Does it merely detect that tampering has occurred, does it prevent tampering entirely or does it simply make tampering more difficult to achieve. It is impossible to divine from the claim language itself what is being claimed. As to its structure, the claim language recites merely that "said protected processing environment including hardware or software."

Other deficiencies can be seen in Claim 34 of the '721 patent. There, the open-ended identification of PPE as "comprising: a first tamper resistant barrier" which itself has a "first security level," a "first secure execution space," and "at least one arrangement" which prevents an identified operation. Conspicuously, this description relies on "secure" and "security." For the reasons noted above, this claim language lends no clarity to PPE but compounds its indefiniteness. Furthermore, one of ordinary skill cannot identify what is being "protected." *See* Mitchell Decl. at 35-37.

In Claim 155 of the '900 patent (Ex. T) InterTrust introduces another coined term "Host Processing Environment" (HPE). While Claim 155 attempts to provide an elaboration of what is meant by HPE through the use of the term "comprising," the description which followed only serves to obscure the meaning and scope of this new term.

While one of ordinary skill in the art reading Claim 155 could surmise that the HPE has at least a central processing unit, main memory and "mass storage," beyond this, the scope and reach of this term is indefinite. The claim goes on to assert that the "mass storage" of the HPE stores "tamper resistant software." This passage fails to set forth with meaningful clarity whether the tamper resistant software is an aspect of the Host Processing Environment. The base description of what *might* be parts of an HPE is insufficient to inform one of ordinary skill in this art as to what the meaningful boundaries and scope of this claim limitation are.

3. THE SPECIFICATION DOES NOT DEFINE THE TERM PROTECTED PROCESSING ENVIRONMENT.

Lacking a context or definition in the claims, the specification must be reviewed for guidance as to the term's meaning. The specification fails as well. InterTrust's first use of the term PPE in the '193 specification states merely that it is one component in a preferred embodiment of a VDE "secure subsystem." Ex. Q, '193 at 9:28. This provides neither information about, nor explanation of, what a PPE is or does. General reference is then made to the PPE in the "Brief Description of the Drawings" but no meaningful discussion, and certainly no definition is provided. '193 at 50:39-41. PPE is not again revisited until Col. 79, ln. 34. Here the patent states that a Host Event Processing Environment (HPE) 655 and Secure Event

Processing Environment (SPE) 503 "may be generically referred to as 'Protected Processing Environments' 650". In Column 105 (at ln. 17-22), the specification states simply that hereinafter in the specification, "unless context indicates otherwise, references to any of 'PPE 650,' 'HPE 655' and 'SPE 503' may refer to each of them." There is no substantive discussion of PPE after this entry.

InterTrust's treatment of PPE is fatally defective for multiple reasons. First, while being a coined term which refers to a feature central to InterTrust's VDE world (*i.e.*, "the invention"), it is never clearly described. At best, InterTrust attempts to give examples of what the "generic" usage of PPE might refer to. Both Secure Event Processing Environments (SPE) and Host Event Processing Environments (HPE) are "environments" which "may be generically referred to as 'Protected Processing Environments' 650". '193 at 79:30-35. In the first instance, InterTrust attempts to illuminate the meaning of a coined term with other coined terms, an unhelpful exercise. As InterTrust's expert identified, SPE and HPE are themselves terms which would not have been known to one of ordinary skill in the art in February 1995.

> Q. Okay. In February 1995, would the person of ordinary skill in the art have been familiar with the term host processing environment?
>
> A. I think not.
>
> Q. In February of 1995, would the person of ordinary skill in the art have been familiar with the phrase secure processing environment?
>
> A. So I have trouble putting my finger on specific usages of that of those three words that I would say were commonplace, but perhaps like protected processing environment, one might—who saw that might assume certain things, but—so I guess my answer would be no, it wasn't a well defined term in the field at the time, but put together they kind of make sense.

Ex. A, Reiter Depo., 134:6-16. Furthermore, there are marked differences between a HPE and SPE rendering the "generic class" to which PPE refers undefined. *See* Mitchell Decl. at 51-53.

To compound the confusion, in many instances where a feature or component of a PPE is set forth, it is qualified with the term "may" indicating that the described feature is optional, hence, may or may not be a part of PPE. This practice further obscures the inherently

ambiguous nature of coined terms. For example, "Protected Processing Environment may refer generally to SPE and/or HPE . . ." (Ex. Q, '193 at 105:18-21). This invariably leaves the relevant public guessing at what might infringe. Such an unconstrained explanation fails to provide sufficient precision.

4. THE TERM HOST PROCESSING ENVIRONMENT IS NOT DEFINED IN THE SPECIFICATION EITHER.

The specification of the '900 patent (Ex. T) does not clear up what the claims leave vague. "Host processing environment" appears initially in the '900 specification in Col. 12 where it is identified that in "some embodiments" certain functions described in the specifications "may be performed by software, for example, in host processing environments of electronic appliances" Ex. T, '900 at 12:27-29 (emphasis added). This introductory use of the term "host processing environment" sheds no light on what it is, what it does or what its parameters are. The term is first used with all initial caps, indicating its coined nature, in Col. 3 at ln. 7, with no accompanying elaboration or definition. Aside from a passing reference in Col. 13, the term is not seen again until Col. 84, ln. 39 where it appears in the simple statement that "another instance of ROS [Rights Operating System] 602 might perform the same task using a *host processing environment* running in protected memory that is emulating a SPU in software." Again, this section of the specification does not elaborate on what the details or constituents of a "host processing environment" are.

As mentioned above with regards to "protected processing environment," the specifications suggest that "host processing environment," "protected processing environment" and "secure processing environment" are terms used as synonyms or as subsets of the other. The mingling of definitions of these coined phrases further aggravates the inherent ambiguity of their use in these patents.

III. ARGUMENT

A. Applicable Legal Standards

The patent statute requires that every patent include "one or more ***claims particularly pointing out and distinctly claiming*** the subject matter which the applicant regards

as his invention." 35 U.S.C. § 112, ¶2 (emphasis added). Patent claims that fail to provide such fair warning are invalid. *Morton Int'l., Inc. v. Cardinal Chem. Co.*, 5 F.3d 1464, 1470 (Fed. Cir. 1993) (affirming holding of patent invalidity because "the claims at issue [were] not sufficiently precise to permit a potential competitor to determine whether or not he is infringing"). The Supreme Court explained the "definiteness" requirement and the "chilling" effect that indefinite patents have on legitimate competition as follows:

> The statutory requirement of particularity and distinctness in claims is met only when they clearly distinguish what is claimed from what went before in the art and clearly circumscribe what is foreclosed from future enterprise. A zone of uncertainty which enterprise and experimentation may enter only at the risk of infringement claims would discourage invention only a little less than unequivocal foreclosure of the field.

United Carbon Co. v. Binney & Smith Co., 317 U.S. 228, 236 (1942). Without abandoning that important principle, the Federal Circuit has made clear that "we have not held that a claim is indefinite merely because it poses a difficult issue of claim construction." *Exxon Research and Eng'g Co. v. United States*, 265 F.3d 1371, 1375 (Fed. Cir. 2001). Summarizing its requirements, the *Exxon* court stated:

> ... what we have asked is that the claims be amenable to construction, however difficult that task may be. If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite... By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of patent validity (citation omitted) and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.

Id. Indefiniteness must be shown by clear and convincing evidence. *L.A. Gear, Inc. v. Thom McAn Shoe Co.*, 988 F.2d 1117 (Fed. Cir. 1993). "The standard of indefiniteness is somewhat high; a claim is not indefinite merely because its scope is not ascertainable from the face of the claims." *Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1342 (Fed. Cir. 2003). While the standard is high, "compliance with the written description requirement is essentially a fact-based inquiry that will "necessarily vary depending on the nature of the invention claimed." Quoting *Enzo Biochem v. Gen-Probe, Inc.*, 296 F.3d 1316, 1324 (Fed. Cir. 2002) (internal citation omitted). *Id.* at 1330 (affirming finding of indefiniteness). Further, "it is not [the court's]

function to rewrite claims to preserve their validity." *Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1349 (Fed. Cir. 2002).

1. Claim Indefiniteness Requires a Two-Part Test

The test for determining whether a claim is definite is "whether those skilled in the art would understand the scope of the claim when the claim is read in light of the rest of the specification." *Union Pac. Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684 (Fed. Cir. 2001); *Morton*, 5 F.3d at 1470. The Federal Circuit has identified two parts to this test: 1) the patent claim, read in light of the rest of the patent and its Patent Office file, must "'reasonably apprise those skilled in the art'" as to its scope; and, 2) the patent claim must be "'as precise as the subject matter permits.'" *Amgen, Inc. v. Chugai Pharmaceutical Co.*, 927 F.2d 1200, 1217 (Fed. Cir. 1991), *quoting Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, 758 F.2d 613, 624 (Fed. Cir. 1985). InterTrust's patents fail both parts of the test, as demonstrated by both the intrinsic and extrinsic evidence.

2. "Secure" and Its Variants Are Indefinite Terms That Render the Claims Containing Them Invalid

The evidence is overwhelming that "secure" lacks a definite meaning in the art. It is a general term that both parties' experts and every third-party witness agree is vague unless given substantial context. InterTrust never provided the needed context in any part of its patents. Accordingly, persons of ordinary skill in the art cannot tell what "secure" means when reviewing the claims. "A claim term is indefinite if it can have more than one meaning to a person of ordinary skill in the art, and the appropriate meaning of the term is not explained in the specification" *See Union Pacific Resources Co. v. Chesapeake Energy Corp.*, 236 F.3d 684, 692 (Fed. Cir. 2001) (finding the term "comparing" indefinite); *In re Cohn*, 58 C.C.P.A. 996, 438 F.2d 989, 993 (CCPA 1971) (finding claim term indefinite where the patentee's conflicting use of the term rendered the scope of the claims uncertain)." *VLT, Inc. v. Artesyn Techs. Inc.*, 238 F. Supp. 2d 339. Here, those of skill in the art, including InterTrust's own expert, have testified that secure can mean countless things to countless different people.

Although words of "degree" and other "relative" terms are sometimes upheld, "when a word of degree is used, the district court must determine whether the patent's specification provides some standard for measuring that degree." *See Seattle Box Company, Inc., v. Industrial Crating & Packaging, Inc.*, 731 F.2d 818, 826 (Fed. Cir. 1984). Here, as shown above, the specification not only fails to provide the necessary context, it adds to the ambiguity. Without some constraining parameters, subjective adjectives like "secure" are indefinite. A predecessor to the Federal Circuit, for example, affirmed the rejection of claims using the "relative" terms "stiff" and "resilient" (describing brush bristles) because the patent provided no guidance as to how stiff or how resilient. *See Application of Lechene*, 277 F.2d 173, 176 (C.C.P.A. 1960). Stiff, unlike "secure," is one-dimensional – the only question was "how stiff?" "Secure" raises not only the question of "how secure," but also, "what kind of security," "from whom," and so on.

Moreover, InterTrust's indexing of "secure" to customer preferences in the specification makes it comparable to a rejected claim brought before the Board of Patent Appeals and Interferences in *Ex parte Brummer*, 12 USPQ2d (BNA) 1653 (BPAI 1989). In *Brummer*, the claim was directed to an improved recumbent bicycle having "a wheelbase that is between 58 percent and 75 percent of the height of the rider that the bicycle was designed for." The Board held that "whether the bicycle was covered by the claim would be determined not on the basis of the structural elements and their interrelationships, as set forth in the claim, but by means of a label placed upon the bicycle at the discretion of the manufacturer." *Id* at **3-4. The Board noted that with such claim language, a claim may be infringed when ridden by one rider, but not when ridden by another. Similarly, because the "level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely," (Ex. Q, '193 at 49:59-62), the scope of the claims depends on unpredictable, ill defined and ever-changing market factors. Indeed, InterTrust's use of "secure" is more indefinite than the language at issue in *Brummer*. In that case, the indefinite language allowed the patentee to vary the meaning of the claims as to one variable (size of the wheelbase); InterTrust's claims apparently seek leeway to shift and remold

themselves along all of the different axes of "security" discussed above.

Finally, secure and its variants further fail the definiteness requirement in failing to be as "precise as the subject matter allows." As demonstrated by its own documentation and by the widespread availability of model security policies, InterTrust had the ability to provide more definite meanings. It did not, and therefore the claim terms are not "as precise as the subject matter permits." *Amgen, Inc. v. Chugai Pharmacetical Co.*, 927 F.2d 1200 at 1217.

Claim indefiniteness is particularly problematic where it derives from "conveniently functional language at the exact point of novelty." *General Electric Co. v. Wabash Appliance Corp.*, 304 U.S. 364, 371-372, 58 S. Ct. 899, 902-03 (1938). As InterTrust's own expert testified, "security" is an "essential aspect" of the alleged invention. Reiter Depo., at 23:21-24:9. Accordingly, although no term should be ambiguous in a patent claim, it is particularly inexcusable that this "core" term be left hopelessly vague. *Exxon Research & Engineering Co. v. United States*, 265 F.3d 1371, 1379 (Fed. Cir. 2001) (fatal for limitations critical to patentability to be indefinite).

B. New Or Coined Terms Must Be Defined Or Otherwise Made Clear.

If the patentee elects to use "a term with no previous meaning to those of ordinary skill in the art ... [i]ts meaning ... must be found somewhere in the patent." *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F.3d 1563, 1568 (Fed. Cir. 1997) (emphasis added). In introducing the coined terms "protected processing environment" and 'host processing environment," InterTrust had a "duty to provide a precise definition" for them. It failed to do so. Accordingly, these terms are indefinite and the claims containing them, invalid.

///

///

///

///

///

///

///

IV. CONCLUSION

For the foregoing reasons, and those set forth in the accompanying Report and Declaration of Professor Mitchell, the Court should grant partial summary judgment that the following eleven claims are indefinite and invalid under 35 U.S.C. § 112, ¶ 2: claims 1, 11, and 15 of the '193 patent; claim 2 of the U.S. Patent No. 6, 185,683; claims 1 and 34 of U.S. Patent No. 6,157,721; claim 58 of U.S. Patent No. 5, 920,861; claim 1 of U.S. Patent No. 5, 982,891; claim 155 of U.S. Patent No. 5,892,900; and claims 8 and 35 of U.S. Patent No. 5,917,912.

Dated: March 17, 2003

WILLIAM L. ANTHONY
ERIC L. WESENBERG
KENNETH J. HALPERN
ORRICK, HERRINGTON & SUTCLIFFE LLP

Eric L. Wesenberg
Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION